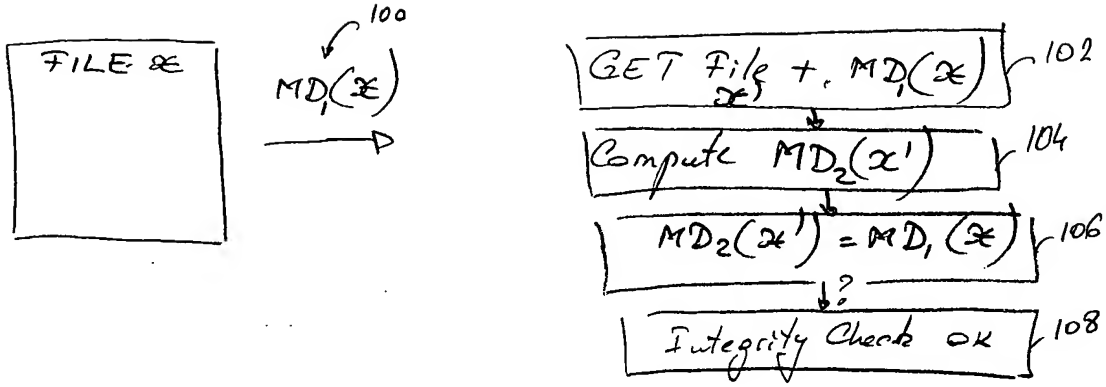

Figure 1 (Prior Art)

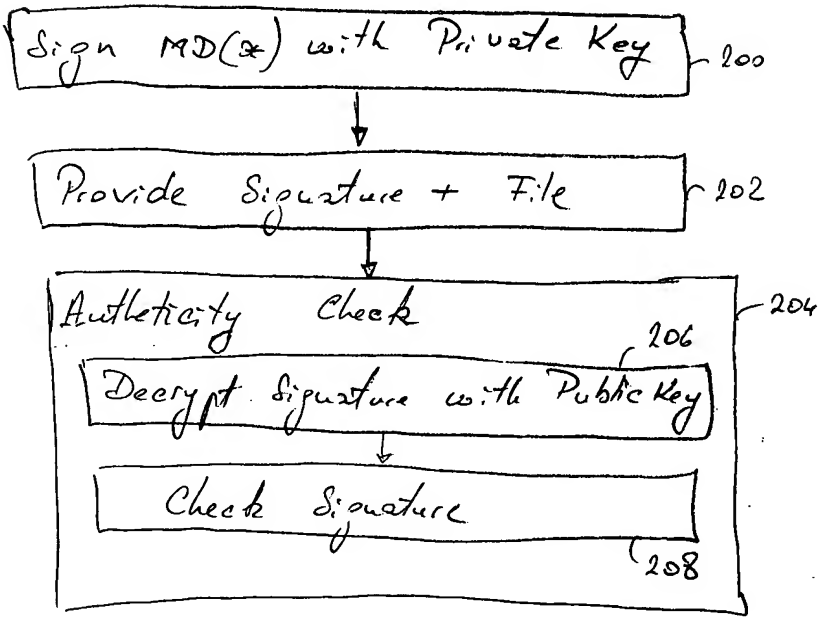

Figure 2 (Prior Art)

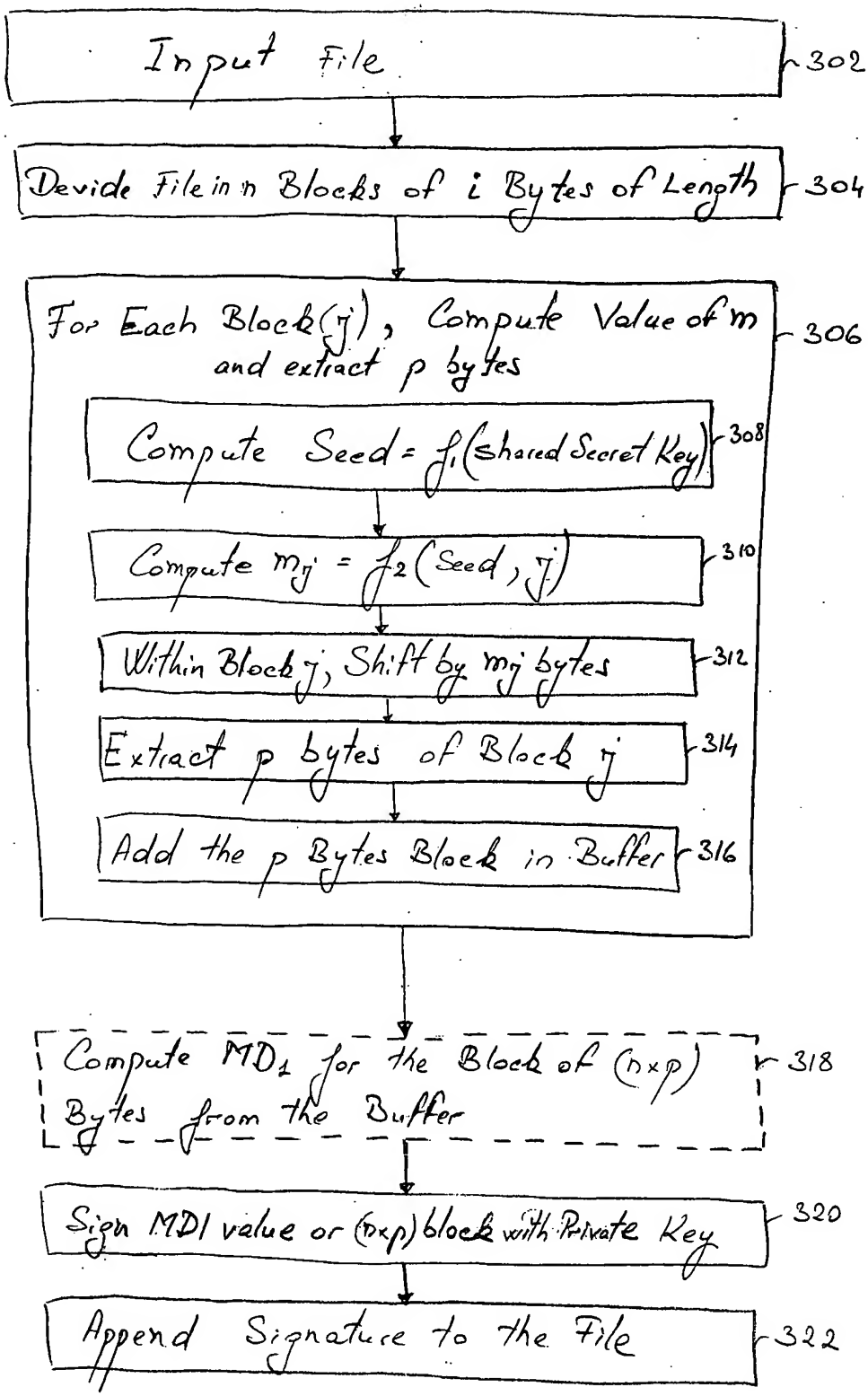
Input File
302
Devide File in n Blocks of i Bytes of Length
304
For Each Block(j), Compute Value of m and extract p bytes
306
Compute Seed = f1(Shared Secret Key)
308
Compute mj = f2(Seed, j)
310
Within Block j, Shift by mj bytes
312
Extract p bytes of Block j
314
Add the p Bytes Block in Buffer
316
Compute MD1 for the Block of (n x p) Bytes from the Buffer
318
Sign MDI value or (n x p) block with Private Key
320
Append Signature to the File
322

Figure 3

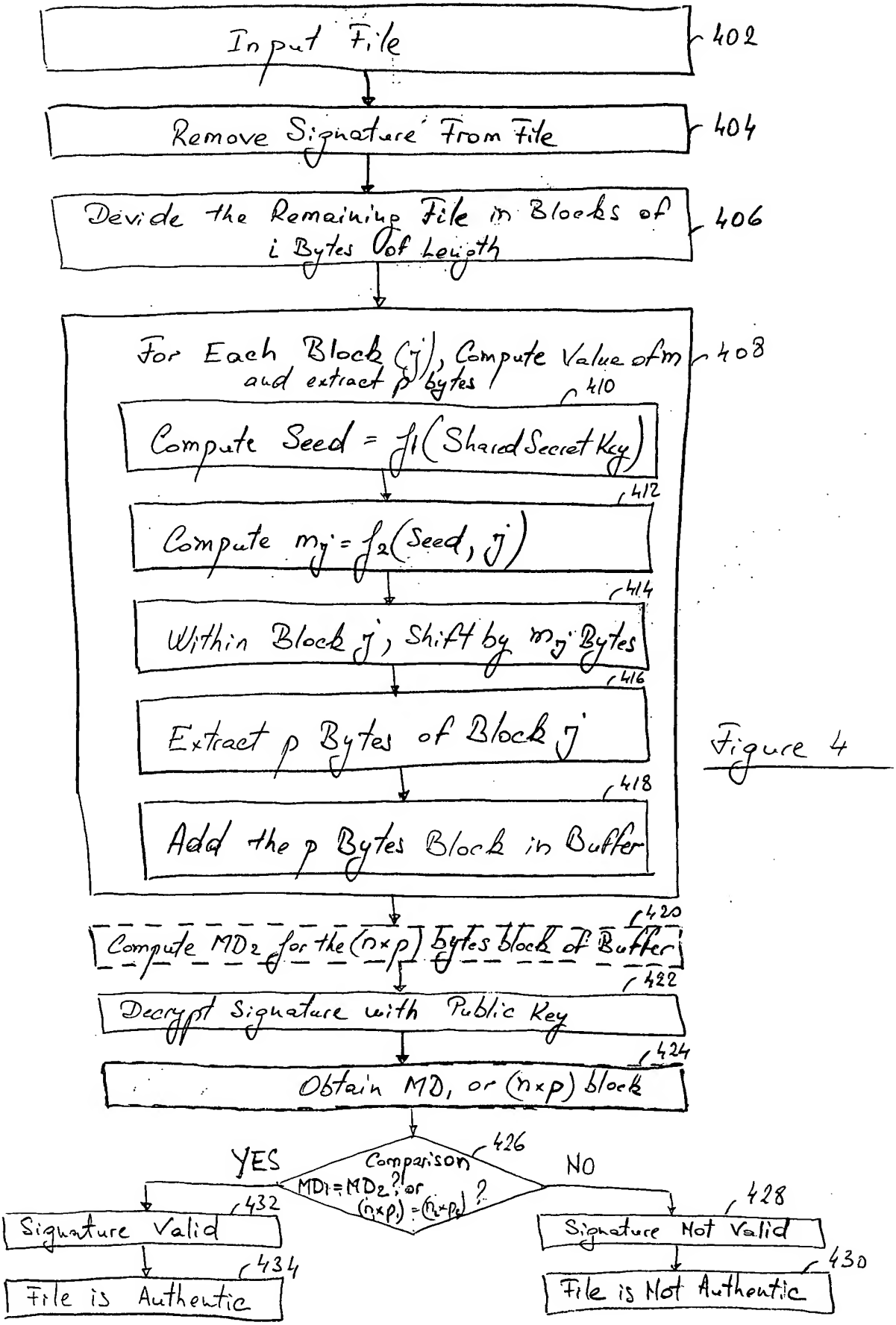
Input File
402
Remove Signature From File
404
Devide the Remaining File in Blocks of i Bytes of Length
406
For Each Block (j), Compute Value of m and extract p bytes
408
Compute Seed = f1(Shared Secret Key)
410
Compute mj = f2(Seed, j)
412
Within Block j, Shift by mj Bytes
414
Extract p Bytes of Block j
416
Add the p Bytes Block in Buffer
418
Compute MD2 for the (n×p) Bytes block of Buffer
420
Decrypt Signature with Public Key
422
Obtain MD1 or (n×p) block
424
Comparison
MD1=MD2 ? or (n×p1)=(n1×p2) ?
426
YES
NO
Signature Valid
432
File is Authentic
434
Signature Not Valid
428
File is Not Authentic
430

Figure 4

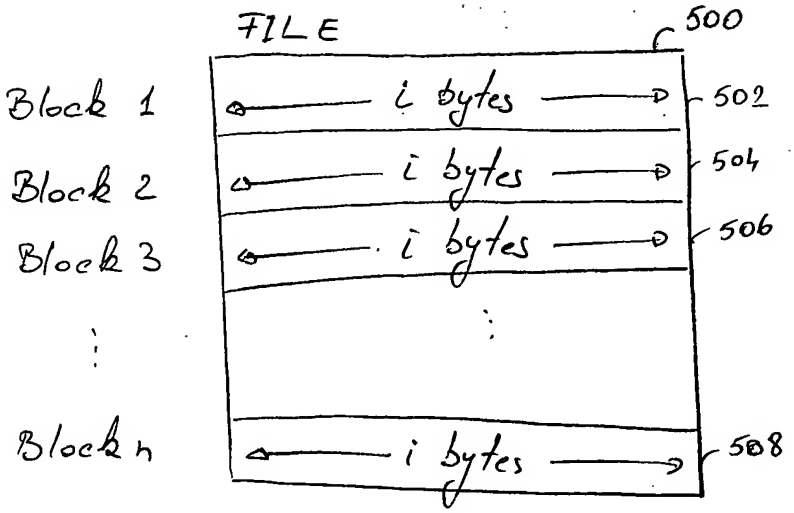

Figure 5

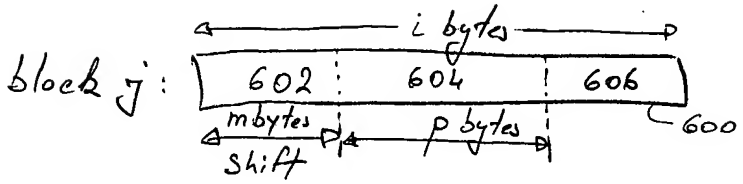

Figure 6

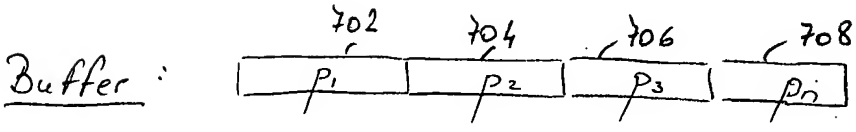

Figure 7

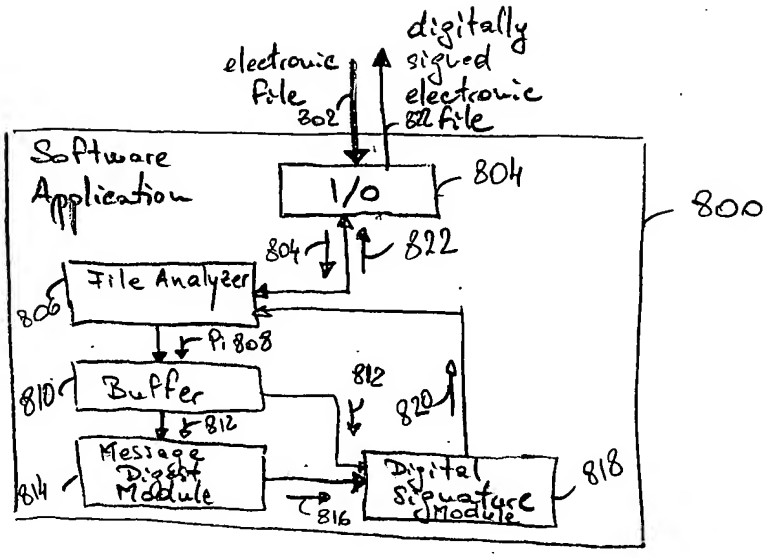

Figure 8

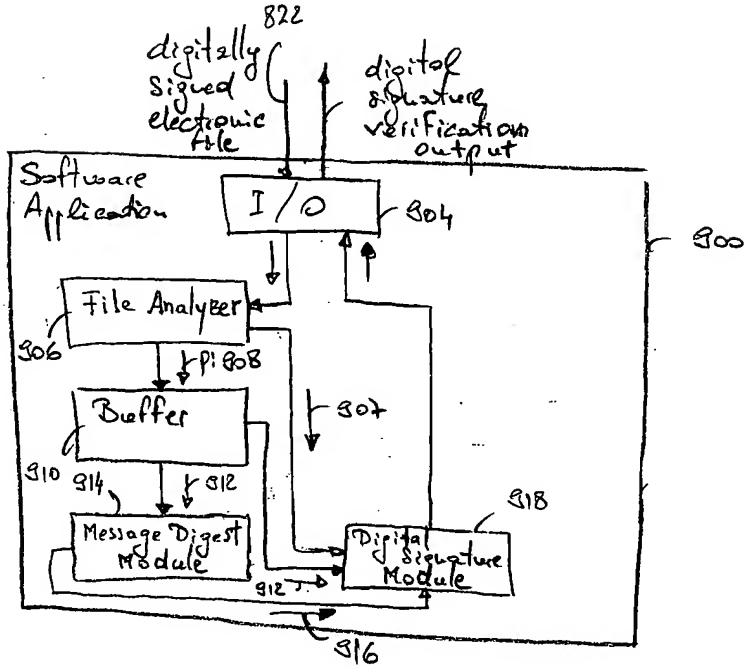

Figure 9